

1. (Currently Amended) A method of generating a pseudo-random number, said method comprising the steps of:
 - a. Establish initialization values for output series of pseudo-random number matrices $X_1 - X_k$;
 - b. Store said initialized pseudo-random number matrices $X_1 - X_k$ in number matrices storage register;
 - b.c. Establish initialization values for variable transition matrices $A_{1,1} - A_{k,1}$;
 - d. Store said initialized transition matrices $A_{1,1} - A_{k,1}$ in transition matrices storage register;
 - e.e. Establish initialization values for variable offset-augmentation matrices $B_{1,1} - B_{j,1}$;
 - f. Store said initialized augmentation matrices $B_{1,1} - B_{j,1}$ in augmentation matrices storage register;
 - g.g. Establish first modulus operators $m_{1,1} - m_{i,1}$;
 - e.h. Retrieve Apply said transition matrices $A_{1,1} - A_{k,1}$ and apply to said output series of pseudo-random number matrices $X_1 - X_k$ to generate a first intermediate matrix value $X_{\text{firsttemp}}$;
 - f.i. Retrieve Apply said offset-augmentation matrices $B_{1,1} - B_{j,1}$ and apply to said first intermediate matrix value $X_{\text{firsttemp}}$ to generate a second intermediate matrix value X_{temp} ; and
 - g.j. Sequentially apply said first modulus operators $m_{1,1} - m_{i,1}$ to said second intermediate matrix value X_{temp} to generate an output value of pseudo-random number matrix X_n ; from which at least one pseudo-random number is extracted.
 - k. Store said first output value matrix X_n in number matrices storage register;
 - l. Retrieve and extract at least one pseudo-random number from element entries of said number matrices storage register; and
 - m. Provide said pseudo-random number to long-term storage register for use in device which can employ pseudo-random numbers.
2. (Currently Amended) A method of generating a plurality of pseudo-random numbers, said method comprising the steps of:
 - a. Establish initialization values for output series of pseudo-random number matrices $X_1 - X_k$;
 - b. Store said initialized pseudo-random number matrices $X_1 - X_k$ in number matrices storage register;
 - b.c. Establish initialization values for variable transition matrices $A_{1,1} - A_{k,1}$;
 - d. Store said initialized transition matrices $A_{1,1} - A_{k,1}$ in transition matrices storage register;
 - e.e. Establish initialization values for variable offset-augmentation matrices $B_{1,1} - B_{j,1}$;
 - f. Store said initialized augmentation matrices $B_{1,1} - B_{j,1}$ in augmentation matrices storage register;
 - g.g. Establish first modulus operators $m_{1,1} - m_{i,1}$;
 - e.h. Retrieve Apply said transition matrices $A_{1,1} - A_{k,1}$ and apply to said output series of pseudo-random number matrices $X_1 - X_k$ to generate a first intermediate matrix value $X_{\text{firsttemp}}$;
 - f.i. Retrieve Apply said offset-augmentation matrices $B_{1,1} - B_{j,1}$ and apply to said first intermediate matrix value $X_{\text{firsttemp}}$ to generate a second intermediate matrix value X_{temp} ;
 - g.j. Sequentially apply said first modulus operators $m_{1,1} - m_{i,1}$ to said second intermediate matrix value X_{temp} to generate a first output value of pseudo-random number matrix X_n ; from which at least one pseudo-random number is extracted;
 - h.k. Store said first output value matrix X_n in said number matrices storage register to establish an updated output series of pseudo-random number matrices $X_{n-k+1} - X_n$;
 - l. Retrieve and extract at least one pseudo-random number from element entries of said number matrices storage register;
 - m. Provide each pseudo-random number to long-term storage register for use in device which can employ pseudo-random numbers;
 - i.n. Retrieve and update said transition matrices $A_{1,1} - A_{k,1}$ through updating process to create and store updated transition matrices $A_{1,2} - A_{k,2}$;
 - j.o. Retrieve Apply said updated transition matrices $A_{1,2} - A_{k,2}$ and apply to said updated output series of pseudo-random number matrices $X_{n-k+1} - X_n$ to generate an updated first intermediate matrix value $X_{\text{firsttemp}}$;

k.p. Retrieve and update said offsetaugmentation matrices $B_{1,1} - B_{j,1}$ through updating process to create and store updated offsetaugmentation matrices $B_{1,2} - B_{j,2}$;

l.q. Retrieve Apply-said updated offsetaugmentation matrices $B_{1,2} - B_{j,2}$ and apply to said updated first intermediate matrix value $X_{firsttemp}$ to generate an updated second intermediate matrix value X_{temp} ;

m.r. Update said first modulus operators $m_{1,1} - m_{i,1}$ through updating process to create updated first modulus operators $m_{1,2} - m_{i,2}$;

n.s. Sequentially apply said updated first modulus operators $m_{1,2} - m_{i,2}$ to said updated second intermediate matrix value X_{temp} to generate a second output value of pseudo-random number matrix X_{n+1} from which at least one pseudo-random number is extracted; and

o.t. Store said second pseudo-random number matrix X_{n+1} in said number matrices storage register-of pseudo-random number matrices..

3. (Currently Amended) A method of generating a plurality of pseudo-random numbers according to claim 2, wherein said steps i.l. through te. are repeated to generate a desired number d of pseudo-random number matrices X_{n+d} from which a plurality of element entries of said pseudo-random number matrices are extracted as pseudo-random numbers are extracted and provided to long-term storage register for use in device which can employ pseudo-random numbers.

4. (Original) A method according to claim 2 further comprising the step of:
Selecting a first subset of said pseudo-random numbers from said updated output series of pseudo-random number matrices.

5. (Original) A method according to claim 1, claim 2, or claim 3, wherein $k = 1$ so that a single variable transition matrix is used.

6. (Currently Amended) A method according to claim 1, claim 2, or claim 3, where $j = 1$ so that a single variable offsetaugmentation matrix is used.

7. (Original) A method according to claim 1, claim 2, or claim 3, where $i = 1$ so that a single modulus operator is used.

8. (Original) A method according to claim 2, further comprising the steps of:
a. Establish second modulus operators $r_{1,1} - r_{g,1}$;
b. Sequentially apply and update second modulus operators $r_{1,1} - r_{g,1}, r_{1,2} - r_{g,2}, \dots r_{1,n+d-k} - r_{g,n+d-k}$ to said updated output series of pseudo-random number matrices to generate a second output series of pseudo-random number matrices.

9. (Currently Amended) A method according to claim 8, further comprising the step of:
Selecting a second subset of said pseudo-random numbers from element entries of said second output series of pseudo-random number matrices.

10. (Original) A method according to claim 1, claim 2, or claim 3:
a. Wherein said first modulus operators $m_{1,1} - m_{j,1}, m_{1,2} - m_{j,2}, \dots m_{1,n+d-k} - m_{j,n+d-k}$ comprise a uniform variable modular reduction, and
b. Further comprising the step of discarding certain pseudo-random numbers which are not uniformly distributed.

11. (Original) A method according to claim 8:
a. Wherein said second modulus operators $r_{1,1} - r_{g,1}, r_{1,2} - r_{g,2}, \dots r_{1,n+d-k} - r_{g,n+d-k}$ comprise a uniform variable modular reduction, and

b. Further comprising the step of discarding certain pseudo-random numbers which are not uniformly distributed.

12. (Currently Amended) A method according to claim 2 or claim 3, further comprising the steps of:

- Create at least one either alternate storage register of pseudo-random number matrices by separately taking steps a – te;
- Create temporary composite pseudo-random number matrices by combining each resulting storage register of pseudo-random number matrices through at least one mathematical operation;
- Create final composite pseudo-random number matrices by applying variable modular reduction to said temporary composite pseudo-random number matrices; and
- Select a subset of pseudo-random numbers from element entries of said resulting final composite pseudo-random number matrices.

13. (Currently Amended) A method according to claim 1, claim 2, or claim 3 further comprising:

- Apply an invertibility evaluation module to each second intermediate matrix value X_{temp} ;
- Adjust offsetaugmentation matrices $B_{1,1} - B_{j,1}, B_{1,2} - B_{j,2}, \dots, B_{1,n+d-1} - B_{j,n+d-1}$, so that said second intermediate matrix value X_{temp} is non-invertible;
- Sequentially apply said first modulus operators $m_{1,1} - m_{i,1}$ to said non-invertible second intermediate matrix value X_{temp} to generate output value of non-invertible pseudo-random number matrix X_n from which at least one pseudo-random number is extracted; and
- Select a subset of pseudo-random number output values from element entries of said non-invertible pseudo-random number matrices.

14. (Currently Amended) An apparatus for generating a pseudo-random number, said apparatus comprising:

- Output matrices initialization means for establishing and storing initialization values for output series of pseudo-random number matrices $X_1 - X_k$ by assigning values to matrix entries;
- Transition matrices initialization means for establishing and storing initialization values for variable transition matrices $A_{1,1} - A_{k,1}$ by assigning values to matrix entries;
- Offset-Augmentation matrices initialization means for establishing and storing initialization values for variable offsetaugmentation matrices $B_{1,1} - B_{j,1}$ by assigning values to matrix entries;
- Modulus operator initialization means for establishing first modulus operators $m_{1,1} - m_{i,1}$ by assigning values to modulus operators;
- First application means for retrieving and applying said transition matrices $A_{1,1} - A_{k,1}$ to said output series of pseudo-random number matrices $X_1 - X_k$ to generate a first intermediate matrix value $X_{firsttemp}$;
- Second application means for retrieving and applying said offsetaugmentation matrices $B_{1,1} - B_{j,1}$ to said first intermediate matrix value $X_{firsttemp}$ to generate a second intermediate matrix value X_{temp} ; and
- Third application means for sequentially applying said first modulus operators $m_{1,1} - m_{i,1}$ to said second intermediate matrix value X_{temp} to generate and store an output value of pseudo-random number matrix X_n from element entries of which at least one pseudo-random number is extracted and provided to long-term storage for use in device which can employ pseudo-random numbers.

15. (Currently Amended) An apparatus for generating a plurality of pseudo-random numbers, said apparatus comprising:

- Output matrices initialization means for establishing and storing initialization values for output series of pseudo-random number matrices $X_1 - X_k$ by assigning values to matrix entries;
- Transition matrices initialization means for establishing and storing initialization values for variable transition matrices $A_{1,1} - A_{k,1}$ by assigning values to matrix entries;

- c. Offset-Augmentation matrices initialization means for establishing and storing initialization values for variable offsetaugmentation matrices $B_{1,1} - B_{j,1}$ by assigning values to matrix entries;
- d. Modulus operator initialization means for establishing first modulus operators $m_{1,1} - m_{i,1}$ by assigning values to modulus operators;
- e.f. First application means for retrieving and applying said transition matrices $A_{1,1} - A_{k,1}$ to said output series of pseudo-random number matrices $X_1 - X_k$ to generate a first intermediate matrix value $X_{\text{firsttemp}}$;
- f.g. Second application means for retrieving and applying said offsetaugmentation matrices $B_{1,1} - B_{j,1}$ to said first intermediate matrix value $X_{\text{firsttemp}}$ to generate a second intermediate matrix value X_{temp} ;
- g.h. Third application means for sequentially applying said first modulus operators $m_{1,1} - m_{i,1}$ to said second intermediate matrix value X_{temp} to generate and store a first output value of pseudo-random number matrix X_n from element entries of which at least one pseudo-random number is extracted and provided to long-term storage for use in device which can employ pseudo-random numbers;
- h.i. Storage means for storing said first output value matrix X_n in a storage register to establish an updated output series of pseudo-random number matrices;
- i.j. Transition matrices updating means for retrieving and updating said transition matrices $A_{1,1} - A_{k,1}$ to create and store updated transition matrices $A_{1,2} - A_{k,2}$;
- j.k. Fourth application means for retrieving and applying said updated transition matrices $A_{1,2} - A_{k,2}$ to said updated output series of pseudo-random number matrices $X_{n-k+1} - X_n$ to generate an updated first intermediate matrix value $X_{\text{firsttemp}}$;
- k.l. Offset-Augmentation matrices updating means for retrieving and updating said offsetaugmentation matrices $B_{1,1} - B_{j,1}$ to create and store updated offsetaugmentation matrices $B_{1,2} - B_{j,2}$;
- l.m. Fifth application means for retrieving and applying said updated offsetaugmentation matrices $B_{1,2} - B_{j,2}$ to said updated first intermediate matrix value $X_{\text{firsttemp}}$ to generate an updated second intermediate matrix value X_{temp} ;
- e.m.n. Modulus operator updating means for updating said first modulus operators $m_{1,1} - m_{i,1}$ to create updated first modulus operators $m_{1,2} - m_{i,2}$;
- n.e. Sixth application means for sequentially applying said updated first modulus operators $m_{1,2} - m_{i,2}$ to said updated second intermediate matrix value X_{temp} to generate a second output value of pseudo-random number matrix X_{n+1} from element entries of which at least one pseudo-random number is extracted and provided to long-term storage register for use in device which can employ pseudo-random numbers; and
- o.p. Second storage means for storing said second pseudo-random number matrix X_{n+1} in said number matrices storage register of pseudo-random number matrices.